What is claimed is:

1. A method for establishing a secure communication between users employing endpoints in a system including one or more security zones, each security zone including one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a caller utilizing a first endpoint in one of said one or more security zones and at least another one of said users is a callee utilizing a second endpoint in one of said one or more security zones, the method including the steps of:

said caller sending a communication request message including a communication request for establishing a secure multimedia communication including security information identifying said caller, via said first endpoint to a first one of said Zone Keepers associated with a security zone including said first endpoint;

said first Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said first Zone keeper determining whether said requested secure communication is an intra-zone or an inter-zone communication:

if said requested communication is an intra-zone communication both said first and second endpoints are in the same security zone, said first Zone Keeper in conjunction with said first and second endpoints in said first security zone establishing said secure communication between said caller and said callee;

if said requested communication is an inter-zone communication said first and second endpoints are in first and second security zones, respectively, said first Zone Keeper sending said request message to said second Zone Keeper associated with said second security zone; and

establishing said secure inter-zone communication utilizing said first Zone Keeper, said first endpoint in said first security zone, said second Zone Keeper and said second endpoint in said second security zone.

2. The method as defined in claim 1 further including providing a capability by each of said Zone Keepers for users of an endpoint in a security zone associated with a particular Zone Keeper to register authentication keys and/or methods and said particular Zone Keeper authenticating said users only through said registered keys and/or methods to honor requests for secure communication.

3. The method as defined in claim 1 further including providing a capability by each of said Zone Keepers to have registered authentication keys and/or methods of endpoints in a security zone associated with a particular Zone Keeper and said particular Zone Keeper authenticating only users authenticated by said user authentication keys and/or methods and said endpoint authentication keys and/or methods to honor requests for secure communication.

4. The invention as defined in claim 1 further including providing a capability by each of said Zone Keepers to have registered by users using an endpoint associated with a particular Zone Keeper individual prescribed security policies and said particular Zone Keeper enforcing said prescribed security policies.

5. The method as defined in claim 1 wherein said intra-zone communication is established by the further steps of

said first Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said first endpoint, said authorization including security information identifying said first Zone Keeper and security information identifying said callee;

said caller authenticating the authorization sent by said first Zone Keeper;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that said callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints in said first security zone, wherein a secure multimedia communication is established.

6. The method as defined in claim 5 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an

authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

7. The method as defined in claim 5 wherein said connection request message includes said communication authorization and security information for authenticating the identity of said callee.

8. The method as defined in claim 7 wherein said connection message further includes a proposal indicating how the caller-callee communication should be set-up.

9. The method as defined in claim 5 further including said first Zone Keeper employing a prescribed security arrangement for authenticating the identity of said caller.

10. The method as defined in claim 9 wherein said prescribed security arrangement includes using a caller identification (ID) and corresponding password.

11. The method as defined in claim 5 wherein said connection request message includes said authorization from said Zone Keeper, security information identifying said caller to said callee and a communication proposal of how the secure caller – callee communication connection is to be set-up.

12. The method as defined in claim 11 wherein said connection request message further includes security information for authenticating the identity of said callee.

13. The invention as defined in claim 11 further including said first Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature and wherein said users authenticate the first Zone Keeper identity by employing said first Zone Keeper's public key.

14. The invention as defined in claim 13 further obtaining said digital signature by said first Zone Keeper signing said request response message with a private-key.

15. The method as defined in claim 1 wherein said inter-zone communication is established by the further steps of

said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone;

said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper;

said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said

authorization message including security information identifying said second Zone Keeper and security information identifying said callee;

said first Zone Keeper authenticating the authorization in said authorization message sent by said second Zone Keeper;

if said authorization in said authorization message is authenticated, said first Zone keeper sending said authorization message to said caller via said first endpoint;

said caller sending, via said first endpoint, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established.

16. The method as defined in claim 15 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

17. The method as defined in claim 15 further including said first Zone Keeper determining whether said caller and said callee are security compatible for the requested secure multimedia communication.

18. The method as defined in claim 17 wherein each of said Zone Keepers has its own private key, and further including said first Zone Keeper signing said communication request message and said second Zone Keeper authenticating that said communication request message was sent by said first Zone Keeper through said first Zone Keeper's private key.

19. The method as defined in claim 18 wherein each of said Zone Keepers has its own digital signature, and further including security information indicating the identity of

said callee and said second Zone Keeper including its digital signature in said authorization message sent to said first Zone Keeper, and said first Zone Keeper authenticating the authorization sent by said second Zone Keeper through the digital signature of said second Zone Keeper.

20. The method as defined in claim 19 wherein each of said Zone keepers has its own public key, said caller authenticates said authorization by verifying said digital signature of said first Zone Keeper and said callee authenticates said authorization and communication proposal by verifying the digital signature of said second Zone Keeper through its public key.

21. The method as defined in claim 1 wherein each of said users has its own password which is registered by the user of an endpoint with the endpoint's associated Zone Keeper, and each of said Zone Keepers has its own private key and its own public key and further including said communication request message including a first prescribed security token, said first Zone Keeper authenticating said first prescribed security token, and if said first prescribed security token is authenticated, determining that said communication should be allowed.

22. The method as defined in claim 21 wherein said intra-zone communication is established by the further steps of

said first Zone Keeper generating a second prescribed security token and a third prescribed security token, inserting said second and third prescribed security tokens in an authentication message and sending said authorization message to said first endpoint, said third prescribed security token including a prescribed challenge value;

said first endpoint authenticating said second prescribed security token in said authorization message and extracting said third prescribed security token;

said first endpoint sending a communication set-up message including said third prescribed security token to said second endpoint;

said second endpoint authenticating said third prescribed security token in said set-up message;

said second endpoint extracting said challenge value from said third prescribed security token and generating a response;

generating a fourth prescribed security token including said response;

said second endpoint sending a call proceeding message including said fourth prescribed security token to said first endpoint;

said first endpoint authenticating said fourth prescribed security token to authenticate said second endpoint; and

if said second endpoint is authenticated, establishing said secure multimedia communication using said first and second endpoints.

23. The method as defined in claim 22 wherein said first prescribed security token is authenticated by employing the password registered by said user of said first endpoint.

24. The method as defined in claim 23 wherein said second and third prescribed security tokens are generated using said Zone Keeper's private-key.

25. The method as defined in claim 24 wherein said second prescribed security token is authenticated by said first endpoint using said Zone Keeper's public-key.

26. The method as defined in claim 25 wherein said third prescribed security token is authenticated by said second endpoint using said Zone Keeper's public-key.

27. The method as defined in claim 26 wherein said response is generated using said registered password of said user of said second endpoint.

28. The method as defined in claim 27 wherein said first prescribed security token is an EPPwdHash security token, said second prescribed security token is a ZKIdenSign security token, said third prescribed security token is a ZKAuthorize security token and said fourth prescribed security token is an EPHashResp security token.

29. The method as defined in claim 21 wherein said inter-zone communication is established by the further steps of

said first Zone Keeper generating a second prescribed security token and including it in a second communication request message;

said first Zone Keeper sending said second communication request message to said second Zone keeper;

said second Zone Keeper determining that said second communication request message from a different security zone than the security zone including said second Zone Keeper, authenticates said second prescribed security token;

if said second Zone Keeper authorizes said communication request in said second communication request message, said second Zone Keeper generating a third prescribed security token and a fourth prescribed security token;

said second Zone Keeper generating a second communication authorization message including said third and fourth prescribed security tokens and sending said second communication authorization message to said first Zone Keeper;

said first Zone Keeper authenticating said fourth prescribed security token and if authenticated generating a fifth prescribed security token and replaces it for said fourth prescribed security token in said second communication authorization message to generate a modified second authorization communication message, and sending said modified second authorization communication message to said first endpoint;

said first endpoint authenticating said fifth prescribed security token in said modified second communication request message;

if said fifth prescribed security token is authenticated, said first endpoint generating a communication set-up message including a sixth prescribed security token including a prescribed challenge value and sending said communication set-up message to said second endpoint;

said second endpoint authenticating said sixth prescribed security token, extracting said prescribed challenge value and generating a response;

generating a seventh prescribed security token including said response;

said second endpoint generating and sending a call proceeding message including said seventh prescribed security token to said first endpoint;

said first endpoint authenticating said responses in said fifth and seventh prescribed security tokens to authenticate said second endpoint; and

if said second endpoint is authenticated, establishing said secure multimedia communication using said first and second endpoints.

30. The method as defined in claim 29 wherein said first prescribed security token is authenticated by employing the password registered by said user of said first endpoint.

31. The method as defined in claim 30 wherein said second prescribed security token is generated using said first Zone Keeper's private-key.

32. The method as defined in claim 31 wherein said second prescribed security token is authenticated by said second Zone Keeper using said first Zone Keeper's public-key.

33. The method as defined in claim 32 wherein said third prescribed security token is generated by said second Zone Keeper using said second Zone Keeper's private-key.

34. The method as defined in claim 33 wherein said fourth prescribed security token is generated by said second Zone Keeper using said second Zone Keeper's private-key.

35. The method as defined in claim 34 wherein said first Zone Keeper authenticates said fourth prescribed security token using said second Zone Keeper's public-key.

36. The method as defined in claim 35 wherein said first Zone Keeper generates said fifth prescribed security token using said first Zone Keeper's private-key.

37. The method as defined as defined in claim 36 wherein said fifth prescribed security token is authenticated by said first endpoint using said first Zone Keeper's public-key.

38. The method as defined in claim 37 wherein said sixth prescribed security token is authenticated by said second endpoint using said second Zone Keeper's public-key.

39. The method as defined in claim 38 wherein said response is generated using said registered password of said user of said second endpoint.

40. The method as defined in claim 39 wherein said first prescribed security token is an EPPwdHash security token, said second prescribed security token is a ZKZKIden security token, said third prescribed security token is a ZKAuthorize security token, said fourth prescribed security token is a second ZKZKIden security token, said fifth prescribed security token is a ZKIdenSign security token, said sixth prescribed security token is a second ZKAuthorize security token and said seventh prescribed security token is an EPHashResp security token.

41. A method for establishing a secure communication between users employing endpoints in a security zone including a plurality of said endpoints and a Zone Keeper,

wherein at least one of said users is a caller utilizing an associated one of said endpoints in said security zone and at least another one of said users is a callee utilizing an associated another of said endpoints in said security zone, the method including the steps of:

said at least one caller sending a communication request message including a communication request for establishing a multimedia communication including security information identifying said caller, via said associated one of said endpoints to said Zone Keeper;

said Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said Zone Keeper sending an authorization message including an authorization of said caller communication request to said caller, via said associated one of said endpoints, said authorization including security information identifying said Zone Keeper and security information identifying said callee;

said caller authenticating the authorization sent by said Zone Keeper;

said caller sending, via said associated one of said endpoints, a connection request message including a communication proposal for establishing a multimedia communication connection with said callee, via said associated another of said endpoints;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said associated another of said endpoints, to said caller via said associated one of said endpoints, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said associated one of said endpoints and said associated another of said endpoints, wherein a secure multimedia communication is established.

42. The method as defined in claim 41 further including, if said Zone Keeper rejects said communication request from said caller, said Zone Keeper sending an

authorization rejected message indicating that said communication request was rejected to said caller, via said associated one of said endpoints.

43. The method as defined in claim 41 wherein said connection request message includes said communication authorization and security information for authenticating the identity of said callee.

44. The method as defined in claim 43 wherein said connection message further includes a proposal indicating how the caller-callee communication should be set-up.

45. The method as defined in claim 41 further including said Zone Keeper employing a prescribed security arrangement for authenticating the identity of said caller.

46. The method as defined in claim 45 wherein said prescribed security arrangement includes using a caller identification (ID) and corresponding password.

47. The method as defined in claim 41 wherein said connection request message includes said authorization from said Zone Keeper, security information identifying said caller to said callee and a communication proposal of how the secure caller – callee communication connection is to be set-up.

48. The method as defined in claim 47 wherein said connection request message further includes security information for authenticating the identity of said callee.

49. The method as defined in claim 48 further including providing a capability by said Zone Keeper for users of an endpoint in said security zone to register authentication keys and/or methods and said Zone Keeper authenticating said users only through said registered keys and/or methods to honor requests for secure communication.

50. The method as defined in claim 49 further including providing a capability by said Zone Keeper to have registered authentication keys and/or methods of endpoints in said security zone and said Zone Keeper authenticating only users authenticated by said user authentication keys and/or methods and said endpoint authentication keys and/or methods to honor requests for secure communication.

51. The invention as defined in claim 47 further including providing a capability by said Zone Keeper to have registered by users individual prescribed security policies and said Zone Keeper enforcing said prescribed security policies.

52. The invention as defined in claim 47 further including said Zone Keeper providing authentication of its identity by using public-key cryptography and a digital signature and wherein said users authenticate the Zone Keeper identity by employing said Zone Keeper's public key.

53. The invention as defined in claim 52 further obtaining said digital signature by said Zone Keeper signing said request response message with a private-key.

54. A method for establishing a secure communication between users employing endpoints in a system including one or more security zones, each security zone including one or more of said endpoints and a Zone Keeper, wherein at least one of said users is a caller utilizing a first endpoint in one of said one or more security zones and at least another one of said users is a callee utilizing a second endpoint in one of said one or more security zones, the method including the steps of:

said caller sending a communication request message including a communication request for establishing a secure multimedia communication including security information identifying said caller, via said first endpoint to a first one of said Zone Keepers associated with a security zone including said first endpoint;

said first Zone Keeper authenticating the identity of said caller, and if said caller identity is authenticated, authorizing said caller's communication request;

said first Zone keeper determining whether said endpoint being used by said callee is in said first security zone or in a second one of said security zones;

if it is determined that said second endpoint in said second security, said first Zone Keeper forwarding said communication request message to a second Zone Keeper associated with said second security zone;

said second Zone Keeper authenticating that the communication request message is from said first Zone Keeper;

said second Zone Keeper sending an authorization message including an authorization of said caller communication request to said first Zone Keeper, said authorization message including security information identifying said second Zone Keeper and security information identifying said callee;

said first Zone Keeper authenticating the authorization in said authorization message sent by said second Zone Keeper;

if said authorization in said authorization message is authenticated, said first Zone keeper sending said authorization message to said caller via said first endpoint;

said caller sending, via said associated one of said endpoints, a connection request message including a communication proposal for establishing a secure multimedia communication connection with said callee, via said second endpoint;

said callee authenticating said authorization and said communication proposal;

said callee sending, via said second endpoint, to said caller via said first endpoint, an acceptance message indicating that callee accepts the communication proposal, said message including security information identifying said callee;

said caller authenticating the identity of said callee; and

if said caller authenticates said identity of said callee, establishing said caller and said callee communication through said first and second endpoints, wherein a secure multimedia communication is established.

55. The method as defined in claim 54 further including, if said first Zone Keeper rejects said communication request from said caller, said first Zone Keeper sending an authorization rejected message indicating that said communication request was rejected to said caller, via said first endpoint.

56. The method as defined in claim 54 further including said first Zone Keeper determining whether said caller and said callee are security compatible for the requested secure multimedia communication.

57. The method as defined in claim 56 wherein each of said Zone Keepers has its own private key, and further including said first Zone Keeper signing said communication request message and said second Zone Keeper authenticating that said communication request message was sent by said first Zone Keeper through said first Zone Keeper's private key.

58. The method as defined in claim 57 wherein each of said Zone Keepers has its own digital signature, and further including security information indicating the identity of said callee and said second Zone Keeper including its digital signature in said authorization message sent to said first Zone Keeper, and said first Zone Keeper authenticating the authorization sent by said second Zone Keeper through the digital signature of said second Zone Keeper.

59. The method as defined in claim 58 wherein each of said Zone keepers has its own public key, said caller authenticates said authorization by verifying said digital signature of said first Zone Keeper and said callee authenticates said authorization and communication proposal by verifying the digital signature of said second Zone Keeper through its public key.